

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-110504

(43) 公開日 平成11年(1999) 4月23日

(51) Int.Cl. ⁹	識別記号	F I	
G 0 6 K 17/00		G 0 6 K 17/00	T
			D
			L
B 4 2 D 15/10	5 2 1	B 4 2 D 15/10	5 2 1
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 B
審査請求 未請求 請求項の数 6 O L (全 8 頁) 最終頁に続く			

(21) 出願番号 特願平9-267324

(22) 出願日 平成9年(1997) 9月30日

(71) 出願人 000003193

凸版印刷株式会社

東京都台東区台東1丁目5番1号

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 山岡 憲一

東京都台東区台東1丁目5番1号 凸版印刷株式会社内

(72) 発明者 平野 誠治

東京都台東区台東1丁目5番1号 凸版印刷株式会社内

(74) 代理人 弁理士 川▲崎▼ 研二

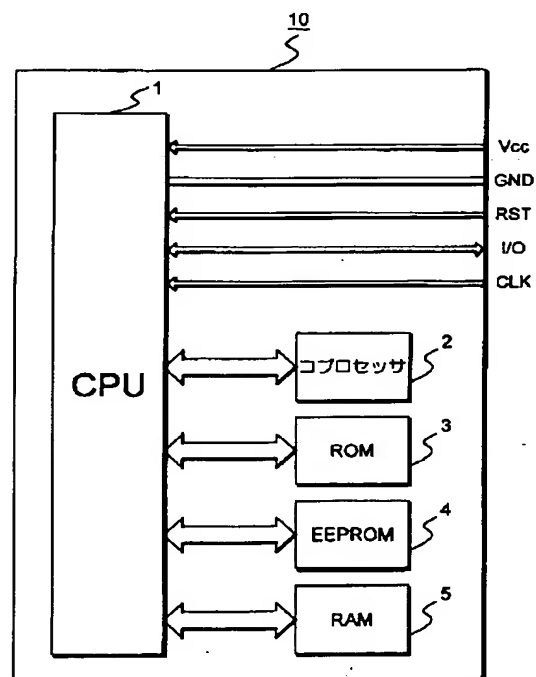
最終頁に続く

(54) 【発明の名称】 ICカード

(57) 【要約】

【課題】 電子現金等のシステムで用いられた場合でも、各種データについての処理時間が短く、セキュリティ性の高いICカードを提供する。

【解決手段】 RAM 5 または EEPROM 4 には、金融取引等についてのデータが複数のレコードに分割して格納してある。CPU 1 は、その複数のレコードを所定のレコード数毎に結合してデータのかたまりをつくる。そして、CPU 1 は、その結合したデータのかたまり毎に圧縮処理および暗号化処理を行う。そして、CPU 1 は、その圧縮処理および暗号化処理した結果をRAM 5 またはEEPROM 4 に格納するとともに、署名データとして端末装置側へ送出する。ここで、コプロセッサ 2 は、暗号化処理におけるべき乗剰演算を行う。



【特許請求の範囲】

【請求項1】 外部装置と接続され、書き換え可能なメモリ手段と、外部からの命令に基づいてデータ処理を行う演算手段を有するICカードにおいて、前記メモリに格納されているデータであって複数のレコードに分割してあるデータを、所定数のレコード毎に1個のブロックに結合する結合手段と、前記結合手段が結合したブロック毎に連続して当該データをデータ圧縮をする圧縮手段と、前記圧縮手段によって圧縮したデータを前記メモリに格納する格納手段と、前記格納手段によって格納したデータを所定の暗号方式で暗号化することで署名データを生成する署名データ生成手段とを具備することを特徴とするICカード。

【請求項2】 請求項1記載のICカードにおいて、前記署名データを不揮発的に保持する署名データ保持手段を有することを特徴とするICカード。

【請求項3】 請求項1または2記載のICカードにおいて、前記署名データ生成手段は、べき乗剰余演算が可能なコプロセッサを用いて暗号化の処理をすることを特徴とするICカード。

【請求項4】 請求項1、2または3記載のICカードにおいて、前記圧縮手段は、一方向性ハッシュ関数を用いてデータ圧縮することを特徴とするICカード。

【請求項5】 請求項1、2、3または4記載のICカードにおいて、前記署名データ生成手段における暗号方式は、公開型暗号方式であることを特徴とするICカード。

【請求項6】 請求項1、2、3、4または5記載のICカードにおいて、前記メモリに格納されているデータであって複数のレコードに分割してあるデータは、取引の履歴の一部を示す取引データを含むことを特徴とするICカード。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、電子現金等を取り扱うシステムで用いられるICカードに関する。特に本発明は、取引の履歴を示すデータであるLOGデータを用いてICカード内で署名データを生成して、取引データの認証をするICカードに関する。

【0002】

【従来の技術】 ICカードは、例えば、セキュリティ性を確保しなければならない金融取引システム（電子現金システム）に用いられる。この種のICカードでは、商取引の状態（日時、場所、金額など）を示す取引データを取り扱い、また、セキュリティ性を高めるため暗号化した署名データを用いてその取引についての認証を行うようにしている。

【0003】 ところで、従来においては、署名データは、ICカード内に格納されているデータを端末装置側で読み出し、これを暗号化して再度ICカードに格納していた。ここで、端末装置側とは、ICカードの通信相手となる装置であって、金融取引システムなどにおける上位システムをいう。また、取引データについては、1レコードについて暗号化してTAC（Transaction Authentication Code）を生成し、これをICカードに格納していた。この場合、取引データが複数のデータによって構成されるときは、レコード毎にTACを生成し、ICカードに格納するか、端末装置側で取引データを圧縮し、暗号化した後にICカードに格納していた。

【0004】 なお、TACとは、DES（Data Encryption Standard）、FEAL（Fast Data Encryption Algorithm）利用の認証子生成検査法による暗号をいう。ここで、DESとは、アルゴリズム公開型の共通鍵方式の暗号方式をいう。共通鍵方式とは、復号鍵が暗号化鍵に等しいか暗号化鍵から簡単に導ける暗号方式をいい、対称暗号系ともいう。共通鍵方式は、比較的小規模のプログラムやハードウェアを用いても高速な処理が可能で、実用性の高いものを構成しやすい。

【0005】

【発明が解決しようとする課題】 ところで、従来のICカードにおいては、レコード単位にMACを生成するので、複数のレコードからなる取引データ（日時、場所、金額等）についてはMAC生成を複数回行う必要があった。

【0006】 また、端末装置側でICカードを使用するときは、セキュリティ性を高めるためにMACデータを8バイトの長いデータにする。そして、複数のレコードをICカードに格納する場合は、各レコード毎に長いMACデータが付加されているので、ICカードが内蔵するメモリの使用量を増大させてしまう。また、この場合は、そのメモリの内容においてMACデータ以外の取引データの割合が少なくなり、ICカードのメモリの有効利用上も問題があった。

【0007】 本発明は、このような背景の下になされたものであり、認証用データ等を少ない記憶容量で効率的に記憶することができるとともに、セキュリティ性の高いICカードを提供することを目的とする。

【0008】

【課題を解決するための手段】 上述した課題を解決するために、請求項1記載の発明は、情報を書き換え可能に格納するメモリと、前記メモリに格納されているプログラムに基づいて当該ICカードの動作を制御する中央処理装置とを具備するICカードにおいて、前記メモリに格納されているデータであって複数のレコードに分割してあるデータを、所定数のレコード毎に1個のブロックに結合する結合手段と、前記結合手段が結合したブロック毎に連続して当該データをデータ圧縮をする圧縮手段

と、前記圧縮手段によって圧縮したデータを前記メモリに格納する格納手段と、前記格納手段によって格納したデータを所定の暗号方式で暗号化することで署名データを生成する署名データ生成手段とを具備することを特徴とする。

【0009】また、請求項2記載の発明は、請求項1記載のICカードにおいて、前記署名データを不揮発的に保持する署名データ保持手段を有することを特徴とする。

【0010】また、請求項3記載の発明は、請求項1または2記載のICカードにおいて、前記署名データ生成手段は、べき乗剰余演算が可能なコプロセッサを用いて暗号化の処理をすることを特徴とする。

【0011】また、請求項4記載の発明は、請求項1、2または3記載のICカードにおいて、前記圧縮手段は、一方向性ハッシュ関数を用いてデータ圧縮することを特徴とする。

【0012】また、請求項5記載の発明は、請求項1、2、3または4記載のICカードにおいて、前記署名データ生成手段における暗号方式は、公開型暗号方式であることを特徴とする。

【0013】また、請求項6記載の発明は、請求項1、2、3、4または5記載のICカードにおいて、前記メモリに格納されているデータであって、複数のレコードに分割してあるデータは、取引の履歴の一部を示す取引データを含むことを特徴とする。

【0014】

【発明の実施の形態】以下、図面を参照して、この発明の実施形態について説明する。

A：実施形態の構成

図1は、本発明の一実施形態であるICカードの構成を示すブロック図である。図において、1は装置各部を制御するCPUであり、2は暗号化処理におけるべき乗剰余演算をするコプロセッサである。3は、CPU1の動作を規定するプログラムなどを記憶するROMであり、EEPROM4はデータを書き換え可能に記憶する不揮発性メモリである。なお、CPU1の動作を規定するプログラムはEEPROM4に記憶させてもよい。RAM5は、データを一時的に格納する揮発性メモリである。

【0015】CPU1は、ICカード10が端末装置（図示せず）に挿入された状態において、電源Vcc、クロックCLK、リセット信号RSTおよびグランド電位GNDが与えられるようになっている。また、CPU1は、端末装置とICカード10との間の双方におけるデータの授受をI/O端子を介して行う。

【0016】RAM5またはEEPROM4の一部は、CPU1が各種の情報処理をする際の作業バッファともなる。さらにRAM5またはEEPROM4の一部は、図6に示すようなファイル構造のレコードが格納されている。そのレコードは、金融取引または商取引などにおけ

る金額、取引時間、取引場所などの履歴を示すデータなどからなる。

【0017】B：実施形態の動作

次に、上記構成からなるICカード10の動作を説明する。図2は、ICカード10におけるコマンド処理を示すフローチャートである。まず、CPU1は、端末装置側から受けた命令がハッシュコマンドであるか否かを判断する（S1）。ここで、ハッシュコマンドである場合は、図3に示すレコード結合処理及び図4に示す圧縮処理をする（S2）。すなわち、ハッシュコマンドとは、ICカード10の内部において、複数のレコードを結合して、その結合したデータをハッシュ関数で圧縮処理することを要求するコマンドである。

【0018】一方、ステップS1において、ハッシュコマンドでない場合は、CPU1は受けた命令が暗号コマンドであるか否かを判断する（S3）。ここで、暗号コマンドである場合は、暗号認証処理すなわちEEPROM4またはRAM5に格納してあるデータを暗号化して署名データを生成する処理を行う（S4）。ステップS3において、暗号コマンドでない場合、すなわち受けた命令がハッシュコマンドでもなく暗号コマンドでもない場合は不当なコマンドとしてエラーステータスを端末装置側に送る（S5）。

【0019】図3は、ICカード10におけるレコード結合処理及び圧縮処理を示すフローチャートである。以下の処理動作は、主にCPU1が制御する。まず、作業バッファの先頭アドレスを所定のレジスタにセットする（S11）。ここで、作業バッファとは、当該レコード結合処理または圧縮処理を実行する際に用いるメモリ領域であり、本実施形態ではRAM5またはEEPROM4内の一部の領域である。

【0020】そして、ハッシュ処理すなわち圧縮処理で用いる初期データをWORK1にセットする（S12）。ここで、WORK1は、作業バッファの一部であり、前記先頭アドレスに基づいて所定領域が確保されている。次に、レジスタr0に、本レコード結合処理の対象となるレコードの数をセットする（S13）。本レコード結合処理の対象となるレコードは、例えば、金融取引等における金額、取引時間、取引場所などの履歴を示すデータからなる。そして、各レコードは、図6に示すようなファイル構造で、RAM5またはEEPROM4に格納されている。

【0021】次に、レジスタr1に、結合処理の対象となるレコードのレコード番号の初期値として「1」をセットする（S14）。そして、レジスタr2に、作業バッファ内データ長の初期値として、「0」をセットする（S15）。ここで、作業バッファ内データ長とは、作業バッファ内に格納した、すなわち作業バッファ内で既に結合したデータの長さをいう。

【0022】その後、レジスタr3に、レジスタr1で

指定しているレコードのレコード長（バイト数）をセットする（S16）。次に、作業バッファがENDの位置にきているか、すなわち、作業バッファが結合したデータでいっぱいか否かを判断する（S17）。ここで、作業バッファがエンドの位置にきていない場合は、レジスタr1が保持している番号のレコードのデータを読み出し、これを作業バッファに格納する（S18）。ここで、その読み出し対象のレコードのデータ長（バイト数）はレジスタr3に保持されているので、そのレジスタr3の値だけ当該レコードのデータを作業バッファに格納すれば、1レコード分のデータが作業バッファに格納される。すなわち、1つのレコードに含まれるデータ全部を読み出して、作業バッファに格納することで、その作業バッファにおいて各レコードを結合している。

【0023】その後、レジスタr2に、レジスタr2の内容とレジスタr3の内容とを加算した値をセットする。これにより、バッファ内のデータ長がレジスタr2にセットされる。さらに、レジスタr1の内容を「1」増加させて、新たなレジスタr1の内容とする（S19）。これにより、作業対象となるレコード番号が「1」増加する。次に、レジスタr0の内容を「1」減少させて、新たなレジスタr0の内容とする（S20）。そして、レジスタr0の内容が「0」になったか否かを判断し、「0」でない場合は、まだ結合及び圧縮処理をしていないレコードがあるので、ステップS16に戻る（S21）。

【0024】これらのステップS13、20、21の処理によって、本レコード結合処理の対象となるレコードの数だけ、ステップS16から21の処理が繰り返され、各レコードを結合していく。

【0025】ステップS21において、レジスタr0の内容が「0」になった場合は、図4に示すハッシュ処理をする（22）。すなわち、レジスタr0の内容が「0」になったことで、結合処理の対象となるレコードの全てが作業バッファにおいて結合されたことがわかる。そして、その結合したレコードの全体について、ハッシュ処理を1回行いデータ圧縮する。

【0026】一方、ステップS17において、作業バッファがいっぱいになった場合は、レジスタr3の内容から読み出しバイト数を減算して、新しいレジスタr3の内容とする（S24）。これは、読み出し作業バッファにr3バイトずつ格納していくと、作業バッファの大きさに満たないデータが出てくるため、その満たない大きさのデータが（r3－読み出しバイト数）になり、これが次のデータを入れるバッファr3の大きさを示すものである。

【0027】その後、図4に示すハッシュ処理、すなわち圧縮処理をする（S25）。これらは、作業バッファがいっぱいになり、所定量のデータがその作業バッファにおいて結合されたので、その結合されたデータを圧

縮処理するものである。その後、まだハッシュ処理されずに残っているレコードを結合して、圧縮処理をすべくステップS17の処理に移る。

【0028】図4は、ICカード10における圧縮処理を示すフローチャートである。すなわち、本フローチャートは、図3におけるステップS22およびステップS24の各圧縮処理を具体的に示したものである。ここで、バッファWORK1、WORK2は、それぞれ圧縮処理についての作業用のバッファであり、それぞれRAM5内にセットするものとする。なお、その作業用のメモリ領域は、EEPROM4内において確保してもよい。

【0029】まず、初期値をバッファWORK1にセットする（S30）。次に、バッファWORK2に圧縮対象となるデータをセットする（S31）。そして、バッファWORK2にあるデータとバッファWORK1にあるデータとを加え合わせ、その加え合わせたデータをハッシュ関数を用いて圧縮する（S32）。その圧縮したデータは、バッファWORK1にセットする（S33）。また、その圧縮したデータであってバッファWORK1にセットしたデータは、バッファWORK2にあるデータに加え合わせられて、ステップS32における圧縮対象となるデータとなる。その後、作業バッファの先頭アドレスを所定のレジスタにセットし（S34）、ハッシュ処理を終了する。

【0030】なお、圧縮アルゴリズムとしては、一般的に知られている一方向性ハッシュ関数を使用する。その一方向性ハッシュ関数としては、例えば、MD4、MD5、SHA、RIPE-MD等を用いることができる。なお、MD4、MD5における“MD”は、「Message Digest」の略である。また、“SHA”は、「Secure Hash Algorithm」の略である。

【0031】図5は、ICカード10における暗号化処理を示すフローチャートである。まず、キーデータを読み出す（S41）。ここで、キーデータはEEPROM4またはROM3に記憶されている。次に、指定レコードのアドレスを計算する（S42）。次に、EEPROM4またはROM3に記憶してある暗号用データのアドレスをセットする（S43）。次に、キーデータアドレスをセットする（S44）。

【0032】次に、コマンドで指定されたNおよびe（d）でRSA（Rivest Shamir Adleman）方式の暗号化処理を行う（S45）。RSA方式とは、公開鍵暗号方式の一つであり、素因数分解が実際上困難である（例えば512ビット以上の）大きな整数を法とする剰余べき乗を用いる方式である。なお、本発明における暗号化処理は、RSA方式に限定されるものではなく、例えば、DES方式、またはFEAL方式などの他の方式を用いることもできる。

【0033】ここで、暗号化におけるべき乗剰余演算は、コプロセッサ2が行う。これにより、暗号化処理が高速に実行される。そして、暗号化処理が完了した後、そ

の処理結果を署名データとしてEEPROM4に格納する。これとともに、出力バッファに署名データをセットして端末装置側に送出する(S46)。

【0034】図6は、ICカード10内における認証用データについてのファイル構造を示す説明図である。まず、ディレクトリ構造としては、データファイルの先頭アドレスと、RAM5またはEEPROM4に格納されているレコードの数とが格納されている。そして、認証用のデータもディレクトリ構造の一つとして格納されている。一方、圧縮処理および暗号化の対象となる取引データなどは、レコード単位でRAM5またはEEPROM4に格納されている。そして、各レコードには、自身のレコード長がデータとして付加されている。

【0035】図7は、ICカード10に対して端末装置側が送出するコマンドフォーマットを示す説明図である。本図では、ハッシュ処理を指令するハッシュコマンドと、暗号化処理を指令する暗号コマンドが示している。また、各処理が正常に実行されたことを示すレスポンス信号のフォーマットも示している。

【0036】これらにより、本ICカードは、複数のレコードからなる取引データをCPU1が本ICカードの内部で結合し、この結合したデータのかたまり、すなわちブロックについてICカード10の内部で圧縮処理および暗号化処理をして署名データを生成するので、取引データを外部に出力せずに署名データを生成することができる。したがって、本ICカードによれば、金融取引システム等で高いセキュリティ性が求められる署名データの偽造および改ざんをほとんど不可能にすることができる。

【0037】また、本ICカードでは、複数のレコードを結合したデータのかたまりについて圧縮処理および暗号化処理をするので、各レコード毎に圧縮処理および暗号化処理をした場合よりもMACデータ等を少なくすることができる。これは、以下の理由による。各レコード毎に暗号化処理をすると各レコード毎にMACデータ等が付与される。一方、データのかたまりについて暗号化処理をするとそのかたまりに1個のMACデータが1つ付与されるだけであるからである。したがって、本ICカードは、そのICカードに内蔵するメモリを効率的に使用することができる。

【0038】また、本ICカードでは、複数のレコードを結合したデータのかたまりについて圧縮処理および暗号化処理をして署名データを生成するので、各レコード毎に圧縮処理および暗号化処理をして署名データを生成した場合よりも圧縮処理および暗号化処理の回数を大幅に低減することができる。したがって、本ICカードは、署名データの生成を高速に実行することができる。

【0039】C：変形例

上述の実施形態においては、複数のレコードを1個のブロックに結合し、そのブロック毎に圧縮処理および暗号化処理をしている。しかし、本発明は上述の実施形態に限定されるものではない。例えば、複数のレコードを1個のブロックに結合し、そのブロックを複数生成し、複数のブロックを1個のブロック集合に結合して、そのブロック集合毎に圧縮処理および暗号化処理を行ってもよい。

【0040】

【発明の効果】以上説明したように、本発明によれば、複数のレコードを1個のブロックに結合し、さらにそのブロック毎に連続して圧縮してから暗号化して署名データを生成する手段をICカード自身がもつので、取引データを前記レコードに含ませた場合でも、その取引データを外部に出力せずに、ICカードの内部で署名データを生成することができ、セキュリティ性の高いICカードを提供することができる。すなわち、本発明によれば、署名データの偽造および改ざんがほとんど不可能となるICカードを提供することができる。

【0041】また、本発明によれば、複数のレコードを結合したブロック毎に、圧縮処理および暗号化処理をするので、各レコード毎に圧縮処理および暗号化処理をした場合よりもMACデータ等を少なくすることができ、ICカードに内蔵するメモリを効率的に使用することができる。

【図面の簡単な説明】

【図1】 本発明の実施形態によるICカードの構成を示すブロック図である。

【図2】 同実施形態におけるコマンド処理を示すフローチャートである。

【図3】 同実施形態におけるレコード結合処理を示すフローチャートである。

【図4】 同実施形態における圧縮処理を示すフローチャートである。

【図5】 同実施形態における暗号化処理を示すフローチャートである。

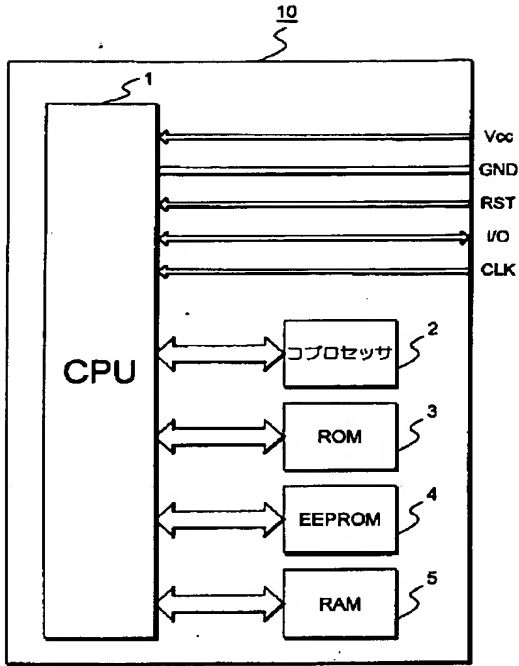
【図6】 同実施形態におけるファイル構造を示す説明図である。

【図7】 同実施形態におけるコマンドフォーマットを示す説明図である。

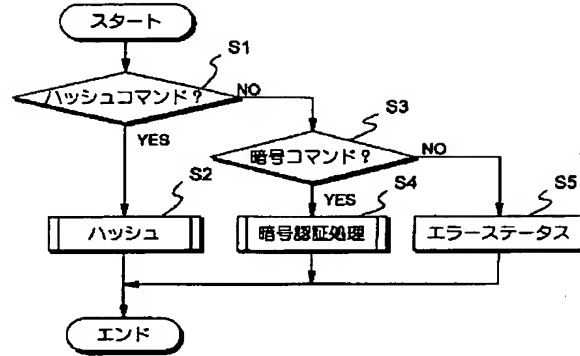
【符号の説明】

- 1 CPU
- 2 コプロセッサ
- 3 ROM
- 4 EEPROM
- 5 RAM

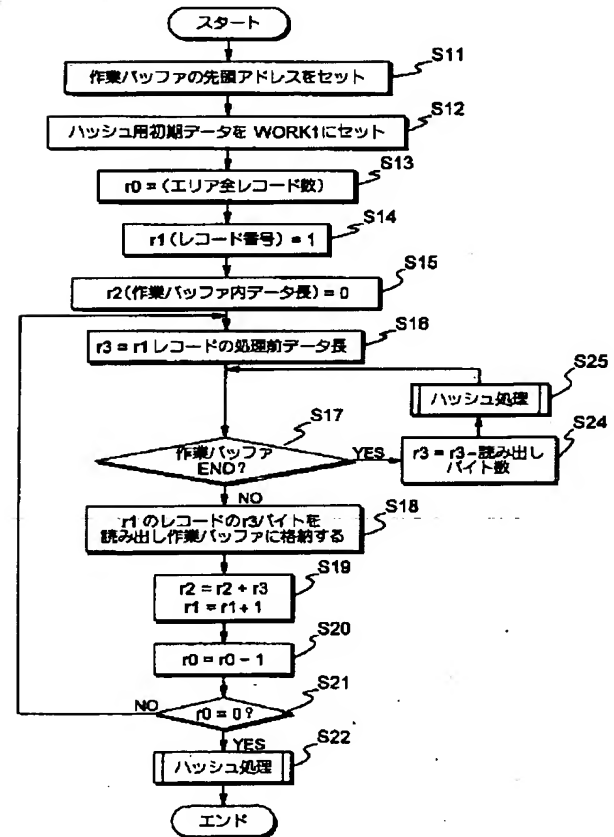
【図1】



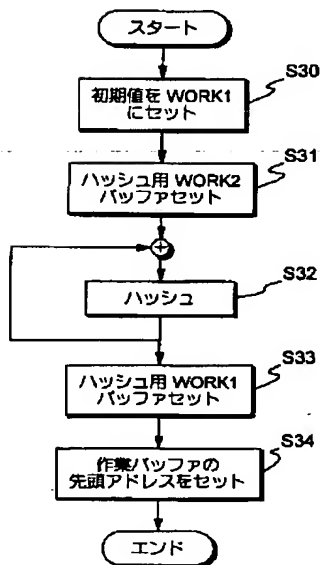
【図2】



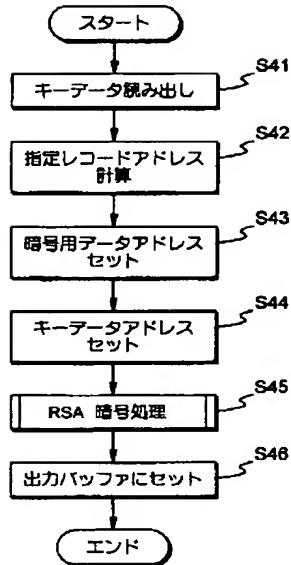
【図3】



【図4】



【図5】



【図6】

ディレクトリ構造

データ先頭アドレス	レコード数	認証用データ	BCC
(2)	(1)	(20)	(1)

レコード数	8バイト	BCC
	16バイト	
	24バイト	
(1)		(1)

【図7】

HASH コマンド

INS	P1	P2
30H	00H	**H
(1)	(1)	(1)

P2: EFID 指定

レスポンス (正常)

STS1	STS2
90H	00H

暗号コマンド

INS	P1	P2	Le
31H	**H	**H	40H
(1)	(1)	(1)	(1)

P1: レコード番号指定

P2: EFID 指定

Le: 期待される認証データ長 (40H)

レスポンス (正常)

認証データ (40H バイト)	STS1	STS2
	90H	00H

フロントページの続き

(51) Int. Cl. 6
G 0 9 C 1/00

識別記号
6 4 0

F I
G 0 9 C 1/00 6 4 0 B

(72) 発明者 高山 文博
東京都台東区台東1丁目5番1号 凸版印刷株式会社内

(72) 発明者 大間 康之
東京都新宿区西新宿3丁目19番2号 日本電信電話株式会社内

(72) 発明者 八田 義洋
東京都新宿区西新宿 3 丁目 19 番 2 号 日本
電信電話株式会社内

(72) 発明者 平田 真一
東京都新宿区西新宿 3 丁目 19 番 2 号 日本
電信電話株式会社内